Environment and classical channels in categorical quantum mechanics

Bob Coecke and Simon Perdrix *

Oxford University Computing Laboratory
CNRS, Laboratoire d'Informatique de Grenoble

coecke@comlab.ox.ac.uk / simon.perdrix@imag.fr

Abstract. We present a both simple and comprehensive graphical calculus for quantum computing. In particular, we axiomatize the notion of an *environment*, which together with the earlier introduced axiomatic notion of classical structure enables us to define classical channels, quantum measurements and classical control. If we moreover adjoin the earlier introduced axiomatic notion of complementarity, we obtain sufficient structural power for constructive representation and correctness derivation of typical quantum informatic protocols.

1 Introduction

Categorical semantics for quantum protocols provides a new perspective on quantum information processing. Particularly appealing is the fact that the symmetric monoidal language comes with an intuitive Penrose-Joyal-Street graphical calculus [33,29]. This approach has meanwhile led to new results in quantum information and quantum foundations. For example, Duncan and the 2nd author have studied graph states, a key resource for the measurement based quantum computational model, and they characterized translations to the circuit model [26,27]. Kissinger and the 1st author have crafted a compositional framework for studying the structure of multipartite quantum entanglement [16]. Edwards, Spekkens and the 1st author have cast quantum theory as well as Spekkens' toy theories within a single mathematical framework, and have performed a corresponding analysis of quantum non-locality in terms of 'phase groups' [15]. Abramsky proved a no-cloning theorem for a very general class of theories [1].

Meanwhile there also exists a software tool with not only a graphical interface but also a 'graphical internal logic', `quantomatic` [24], which (semi-)automates graphical reasoning. It has been developed in a collaboration between Edinburgh (Dixon) and Oxford (Duncan, Kissinger and Merry), and involved interpreting theories formulated in symmetric monoidal language in terms of 'open graphs'

* Work supported by EP/D072786/1, ONR N00014-09-1-0248 and EU FP6 STREP QICS. John Baez, Aleks Kissinger, Prakash Panangaden, Johan Paulsson, Jamie Vicary and the referees of CSL'10 provided useful feedback on an earlier versions.

[25]. For an important fragment of the graphical language, Selinger has proved a completeness theorem with respect to Hilbert spaces [37].

Categorical quantum mechanics notions relevant for this paper are:

(A) Abramsky and the 1st author proposed dagger compact categories as a means to axiomatize bipartite entangled states, map-state duality, bra-ket duality and unitary operations, by endowing compact categories [30] with an identity-on-objects involution, the dagger-functor [2];

(B) Selinger proposed a construction which assigns to any dagger compact category $\mathbf{C}$ of pure states and operations another dagger compact category $CPM(\mathbf{C})$ of 'mixed states' and 'completely positive maps' [35]; the 1st author axiomatized $CPM(\mathbf{C})$ as a dagger compact category with for every object A a privileged 'maximally mixed state' $\perp_A : \mathrm{I} \to A$ [12];

(C) the 1st author and Pavlovic introduced 'classical structures' as certain Frobenius algebras [8], in order to handle classical data and control [20,21,19];

(D) the 1st author and Duncan axiomatized 'complementarity' (or 'unbiasedness') and were able to construct from this basic quantum logic gates [13,14].

The interaction of these concepts has not been subjected to a detailed study yet. Here, we distill the notion of *environment* out of **(B)**, and by blending it in an appropriate manner with **(C)** we define the notion of *classical channel*; these interact in a particularly nice manner with **(D)** and together they provide a simple and elegant graphical calculus to represent and prove correctness of typical quantum computational protocols e.g. teleportation (including classical control) [6], dense coding [7], and the BB84 and Ekert 91 QKD protocols [28].

Our main point is to show how with very little structural effort one straightforwardly reproduces these non-trivial quantum behaviors. Furthermore, the simple explicit account that we obtain here on the classical-quantum interaction, which substantially simplifies the earlier work in this direction by Paquette, Pavlovic and the 1st author in [19], will enable a fully comprehensive purely diagrammatic study of quantum informatic situations involving complex information flows between the classical and the quantum. It moreover provides novel foundational insights on the nature of this interaction.

Section 2 outlines how we conceive the classical-quantum distinction. Section 3 recalls the notion of *classical structure*, and Section 4 discusses complementary (or unbiasedness) thereof. Section 5 introduces the notion of *environment*, and Section 6 combines environment and classical structure to form a *classical channel*, *measurements* (§6.2) and *control operations* (§6.1), and studies the role of *complementarity* –§6.3 provides an explicit interpretation of the graphical language within Hilbert space quantum mechanics for the specific case of qubits. In Section 7 we derive basic quantum informatic protocols. While we restrict ourselves to pure states and operations, our graphical framework straightforwardly extends to mixed states and operations, as indicated in Section 8.

We assume that the reader is familiar with the basic concepts of quantum computation, such as states, operations, measurement and control. The graphical language for symmetric monoidal categories is surveyed in [36], and a tutorial tailored towards applications in categorical quantum mechanics is [17]. In this context, he reader may also find chapters §2 and §4 of [14] useful.

2 Classicality vs. quantumness

Let $\mathcal{H}$ be a Hilbert space. By a *cloning map* one means an operation

$$U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$$

which is such that for all $|\psi\rangle \in \mathcal{H}$ and some $|0\rangle \in \mathcal{H}$ we have

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle\,.$$

When fixing $|0\rangle$ within the argument we can instead consider

$$\Delta := U(- \otimes |0\rangle) : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$$

rather than U. It is well-known that there exists no cloning map [23,39]. Now, if an operation clones certain pure states, say the basis vectors $\{|i\rangle\}_i$, this does not imply that it clones mixtures of these too; setting $\rho = \sum_i \rho_i |i\rangle\langle i|$ we have:

$$\Delta \circ \rho \circ \Delta = \Delta \circ \left(\sum_i \rho_i |i\rangle\langle i| \right) \circ \Delta = \sum_i \rho_i \Delta \circ (|i\rangle\langle i|) \circ \Delta = \sum_i \rho_i |ii\rangle\langle ii| \neq \rho \otimes \rho\,.$$

However, what we do have is that

$$tr_1(\Delta \circ \rho \circ \Delta) = tr_2(\Delta \circ \rho \circ \Delta) = \rho\,, \tag{1}$$

where tr_1 and tr_2 respectively trace out the first and the second system. For arbitrary completely positive maps $\mathcal{E}$ Eqs. (1) becomes:

$$tr_1(\mathcal{E}(\rho)) = tr_2(\mathcal{E}(\rho)) = \rho\,. \tag{2}$$

Universal validity of Eqs. (2) for a particular completely positive map $\mathcal{E}$ acting on the entire space of all density operators has been referred to as *broadcasting*. But the *no-broadcasting theorem* [4], due to Barnum, Caves, Fuchs, Jozsa and Schumacher, states that only mixed states which share a basis in which they all are diagonal (i.e. mixed states that can be jointly simulated by classical probability distributions) can be broadcast by the same completely positive map.

From the above discussion it follows that broadcastability is a strictly weaker requirement than cloneability. We have:

	pure classical	mixed classical	pure quantum	mixed quantum
broadcastable:	`YES`	<u>`YES`</u>	`NO`	`NO`
cloneable:	`yes`	<u>`no`</u>	`no`	`no`

where by classical we refer to a set of density operators that are diagonal in the same basis. So (not non-cloneability but) non-broadcastability 'identifies' quantum relative to classical, in that classical states, both pure and mixed, can always be broadcast by a single quantum operation, while this is not possible for quantum states that cannot be jointly simulated classically. Now, taking the contrapositive, for us classicality will mean *broadcastability*.

Equivalently, one can also conceive classicality as the result of *decoherence* [40]. Concretely, 'total' decoherence is the completely positive map which erases all non-diagonal elements in the matrix representation of a given basis, that is,

$$\mathcal{D}_{\{|i\rangle\}_i} :: |ij\rangle \mapsto \delta_{ij}|ii\rangle\,, \tag{3}$$

where δ_{ij} is the Kronecker delta. Broadcasting and decoherence are indeed closely related: in the case of the first 'one copies into the environment', while in the case of the second 'one couples to the environment'. *Decoherent* then means invariance under this coupling. Formally, decoherent density operators relative to a fixed $\mathcal{D}_{\{|i\rangle\}_i}$ are exactly those collections of density operators that can be jointly broadcast; they all are diagonal in the basis $\{|i\rangle\}_i$ and hence can be simulated by the classical probability distributions that make up the diagonals.

Summarizing the above:

$$\boxed{\text{classical} := \text{broadcastable} \equiv \text{decoherent}}$$

We will treat 'classicality' as a 'behavior' –i.e. behaves as if it is classical in the above discussed sense– rather than as the specification of the actual physical realization of a system. An important point in this context, already realized in [20,19], is that by taking quantum to be the 'default behavior' within the mathematical universe of all operations, characterization of classical entities can be done in purely diagrammatic terms. In the concrete Hilbert space realization, this means that one only needs to rely on the *multiplicative* tensor product structure as a primitive connective, with no reference to the *additive* vector space structure. One could refer to this as 'classicization', in contrast to the standard notion of 'quantization' where one starts with a classical theory and then freely adjoins the additive vector space structure.

As an example, consider a quantum measurement, which when applied to a quantum system changes the state of that quantum system and produces classical data. Since the resulting quantum state is an eigenstate for that measurement, hence broadcastable, it behaves precisely in the same manner as the classical data does. As a result, in the graphical calculus the classical data and the collapsed state won't be distinguishable once we omit explicit specification wether physically they are either classical or quantum. This ambiguity captures a *feature* of the particular manner in which quantum and classical data interact, namely, that the creation of classical data renders the quantum state in an eigenstate. Of course, if we later apply a non-classical unitary to the resulting quantum state, then we reassert its proper quantumness.

Put in type-theoretic terms, there will be no such thing as a fixed 'classical type' and fixed 'quantum type' in our representation, since we can abstract away over these 'implementation details' without altering the essential structure. Of course, one can add those details in order to connect the graphical language to concrete physical protocols where the classical quantum distinction may be fundamental for the conceptual analysis, for example, in quantum teleportation it is crucial that the classical communication can indeed be realized by purely classical finitary means. In Section 7 we give several examples of protocols that

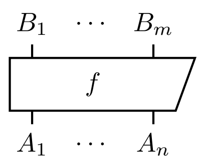
come with specification of what is classical and what is quantum, and then pass to the abstract diagrammatic calculus where forgetting the physical realization is essential to perform the computation.

3 Classical structures

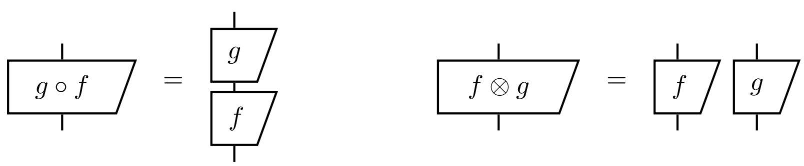
We will work in the graphical representation of symmetric monoidal categories, due to Joyal and Street [29]. Mac Lane's strictification theorem [32, p.257] allows us to take our symmetric monoidal categories to be strict, that is:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \qquad \text{and} \qquad A \otimes \mathrm{I} = A = \mathrm{I} \otimes A\,.$$

Morphisms $f : A_1 \ldots A_n \to B_1 \ldots B_m$, which we interpret as processes are respectively represented as boxes where the input wires represent the objects $A_1 \ldots A_n$ and the output wires represent the objects $B_1 \ldots B_m$:

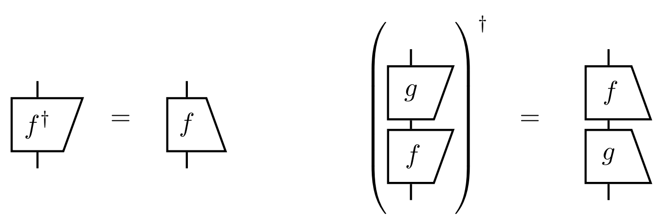


Other shapes may be used to emphasize extra structure. *Elements* $s : \mathrm{I} \to A_1 \ldots A_n$, which in the graphical representation have no inputs, are interpret as 'states', and *co-elements* $e : B_1 \ldots B_m \to \mathrm{I}$ with no outputs are interpreted as 'effects'. In standard quantum notation they would be kets $|\psi\rangle$ and bras $\langle\psi|$ respectively. Composition and tensoring are respectively represented as:



Theorem 1 (Joyal-Street 1991 [29,36]). *An equation follows from the axioms of symmetric monoidal categories if and only if it can be derived in the graphical language via diagram isomorphisms.*

A *dagger functor* on a symmetric monoidal category [35] is an identity-on-objects contravariant involutive strict monoidal functor. It is graphically represented by flipping pictures upside-down, for instance:

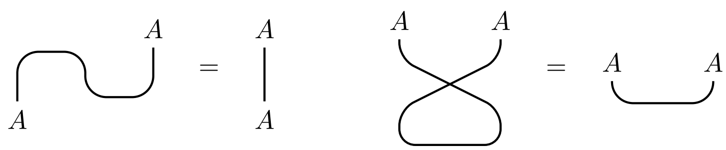


Given such a dagger functor, a morphism $f : A \to B$ is an *isometry* if $f^\dagger \circ f = 1_A$, and it is *unitary* of both f and $f^\dagger$ are isometries.

A *dagger compact category* [3] is a dagger symmetric monoidal category in which each object A comes with two morphisms $\eta_A : \mathrm{I} \to A^* \otimes A$ and $\epsilon_A : A \otimes A^* \to \mathrm{I}$ which satisfy certain equations. In this paper we take all our objects to be *self-dual*, that is, $A = A^*$.[1] Graphically, we represent η_A as:

,

we take ϵ_A to be its dagger, and the equations that govern η_A and ϵ_A are:



Remark 1. The results in this paper can be extended to the case of non-self-dual compact structures, by relying on the results in [18]. This would, for example, be required when considering all three complementary measurements on a qubit.

Theorem 2 (Kelly-Laplaza 1980, Selinger 2007 [30,35]). *An equation follows from the axioms of (dagger) compact categories if and only if it can be derived in the corresponding graphical language via isotopy.*

The key difference between *diagram isomorphism* as in Theorem 1 and *isotopy* as in Theorem 2 is that diagram isomorphisms take specification of the boxes' inputs and outputs into account, while isotopy abstracts away these roles. Hence within the scope of Theorem 2 only the topology of the diagrams matters.

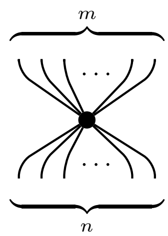
By *classical structures* [20] we mean internal commutative special dagger Frobenius algebras in a dagger compact category for which we also require 'compatibility with the compact structure' (see below). We won't give an explicit definition here, but will rely on a remarkable normal form result that holds for morphisms build from this structure, namely, any morphism

$$\Xi_n^m : \underbrace{A \otimes \ldots \otimes A}_{n} \to \underbrace{A \otimes \ldots \otimes A}_{m}$$

obtained by composing and tensoring the structural morphisms of a classical structure and the symmetric monoidal structure, and of which the diagrammatic representation is connected, only depends on n and m [31]. Graphically

[1] A detailed study of the coherences for this situation is in [38].

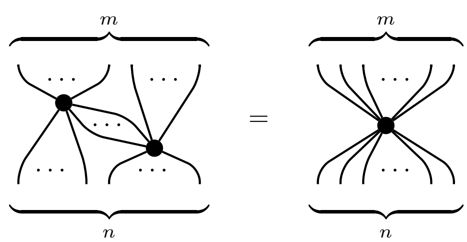
we represent this unique morphism as an $n+m$-*legged spider*:



From the axioms of classical structures it follows that these spiders are invariant when one exchanges the roles of front-legs and back-legs, when one swaps two legs of either of these, and that the $(1+1)$-legged spider is the identity, that is,

$$(\mathit{\Xi}_n^m)^\dagger = \mathit{\Xi}_m^n \qquad \mathit{\Xi}_n^m \circ (1_{A^{\otimes(k)}} \otimes \sigma_{A,A} \otimes 1_{A^{\otimes(n-k-2)}}) = \mathit{\Xi}_n^m \qquad \mathit{\Xi}_1^1 = 1_A\,, \tag{4}$$

where $\sigma_{A,A} : A \otimes A \to A \otimes A$ is the swap map, and, last but not least, that spiders which 'share' legs fuse together, i.e. spiders compose as follows:

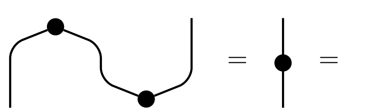


(5)

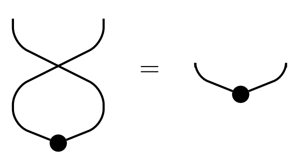
Conversely, the axioms of an internal commutative special dagger Frobenius algebra all follow from Eqs. (4) and (5).

By *compatibility* of the classical structure with a given dagger compact structure we mean that for a spider on A we have $\eta_A = \mathit{\Xi}_2^0$, and consequently that $\epsilon_A = \mathit{\Xi}_0^2$. In graphical terms, that is:

Indeed, for spiders $\mathit{\Xi}_2^0$ and $\mathit{\Xi}_0^2$ we always have:

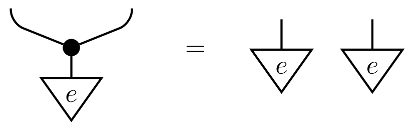


and



that is, they form a dagger compact structure.

In the graphical language we will depict elements (i.e. 'boxes without inputs') by triangles. By a *pure classical element* for a particular classical structure we mean an element which satisfies:



(6)

i.e. it is 'copied'. Below, by e we will only denote such pure classical elements.

In the dagger compact category **FHilb** which has finite dimensional Hilbert spaces as objects, linear maps as morphisms, the tensor product as the monoidal structure, and adjoints as the dagger, classical structures are in bijective correspondence orthonormal bases via this concept of pure classical elements [21]. Concretely, the pure classical elements are exactly the basis vectors, and conversely, given an orthonormal basis $\{|i\rangle\}_i$, the corresponding spiders are the linear maps with as only non-zero action on the basis vectors:

$$\Xi_n^m :: \underbrace{|i\ldots i\rangle}_{n} \mapsto \underbrace{|i\ldots i\rangle}_{m}\,, \tag{7}$$

i.e. arrays of identical basis vectors are mapped on arrays of identical basis vectors, and all other basis vectors are mapped on the zero vector. Important particular examples are

$$\Xi_2^1 :: |ij\rangle \mapsto \delta_{ij}|i\rangle \qquad \text{and} \qquad \Xi_0^1 :: 1 \mapsto \sum_i |i\rangle \tag{8}$$

which define the *multiplication* and its *unit* of the corresponding Frobenius algebra; their adjoints define the corresponding comultiplication and its counit.

Remark 2. In any dagger symmetric monoidal category, the multiplication and its unit suffice to specify a classical structure; one can then construct any other spider by composing Ξ_2^1, Ξ_0^1, $(\Xi_2^1)^\dagger$ and $(\Xi_0^1)^\dagger$ to obtain a morphism with the required number of inputs n and outputs m, that is, the spider Ξ_n^m.

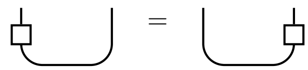
Remark 3. Physically relevant, rather than **FHilb**, is the category WP(**FHilb**) which is obtained by subjecting **FHilb** to the congruence which identifies those linear maps of the same type that are equal up to a complex phase, i.e.

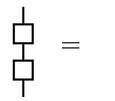
$$f \sim g \;\Leftrightarrow\; \exists\theta \in [0, 2\pi[: f = e^{i\theta}\cdot g\,.$$

The reason is that vectors which are equal up to a complex phase represent the same state in quantum theory. The precise connection between classical structures in **FHilb** and those in WP(**FHilb**) is studied in detail in [14]; roughly put –since this suffices for all practical purposes– classical structures are inherited.

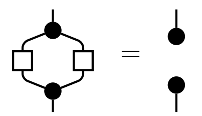
4 Complementary classical structures

Definition 1. A *complementary* endomorphism $H : A \to A$ for a classical structure is a (i) self-conjugate (ii) self-adjoint (iii) unitary endomorphism, graphically,





where self-adjointness is encoded in the symmetry of the small box depicting H, and, which 'transforms a given classical structure into a complementary one', which –following [14]– graphically depicts as:



(9)

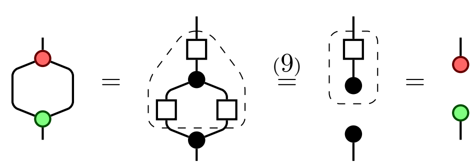
An example of such a complementary morphism is the familiar Hadamard matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

expressed in the basis defined by the classical structure. Rather than axiomatizing a pair of complementary classical structures as in [14], here we axiomatize a morphism which transforms a classical structure in the other one. The defining equation in [14], which involves two classical structures, is obtained by postcomposing both sides of Eq. (9) with H, where

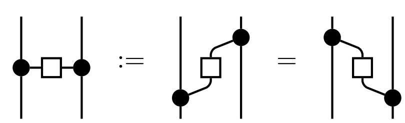
$$\tilde{\Xi}_2^1 := H \circ \Xi_2^1 \circ (H \otimes H) \qquad \text{and} \qquad \tilde{\Xi}_0^1 := H \circ \Xi_0^1$$

then respectively are the multiplication and the unit of the second classical structure. Representing (Ξ_2^1, Ξ_0^1) in green and $(\tilde{\Xi}_2^1, \tilde{\Xi}_0^1)$ in red, we have:

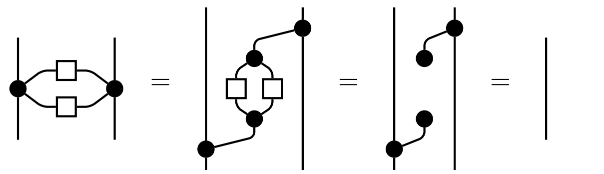


so we recover the characterization of complementarity as in [14]§8.

Remark 4. Since C is self-transposed we can set



By Eq. (9) it then for example follows that:

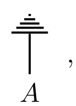


We will use this 'topological trick' throughout this paper.

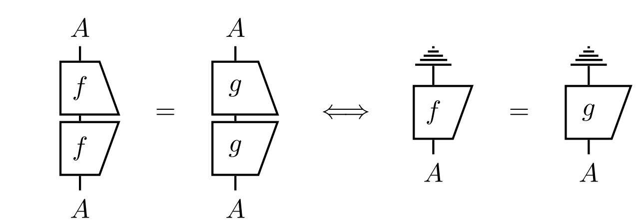
5 Environment

We will consider two dagger compact categories, denoted $\mathbf{C}^{\mathbf{pure}}$ and $\mathbf{C}$ respectively, and we assume that $\mathbf{C}^{\mathbf{pure}}$ is a subcategory of $\mathbf{C}$ which inherits symmetric monoidal structure as well as dagger compact structure, and that $|\mathbf{C}| = |\mathbf{C}^{\mathbf{pure}}|$.

Definition 2. An *environment structure* for $(\mathbf{C}^{\mathbf{pure}}, \mathbf{C})$ consists of a designated co-element $\top_A : A \to \mathrm{I}$ for each object $A \in |\mathbf{C}|$, which we depicted as:



and that for all $A, B \in |\mathbf{C}|$ and all $f, g \in \mathbf{C}^{\mathbf{pure}}(A, B)$ we have



(10)

(11)

We will sometimes abbreviate environment structure to environment.

Remark 5. Eqs. (10,11) had already been introduced in [12], as part of an axiomatization of mixed states and completely positive maps, but it was never considered in relation to classicality, measurements, and complementarity thereof.

Example 1. Let **Dens** be the category with $\mathbb{C}^{n\times n}$ for $n \in \mathbb{N}$ as objects, and with completely positive maps $F : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ as morphisms. A morphism

f is pure, that is, $f \in hom_{\mathbf{Dens^{pure}}}(\mathbb{C}^{n\times n}, \mathbb{C}^{m\times m})$, if there exists a linear map $L : \mathbb{C}^n \to \mathbb{C}^m$ such that $f :: \rho \mapsto L\rho L^\dagger$. Then , the usual trace

$$\top_{\mathbb{C}^{n\times n}} : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n} :: \rho \mapsto tr(\rho)$$

provides an environment structure for $(\mathbf{Dens^{pure}}, \mathbf{Dens})$. Indeed, for any $f :: \rho \mapsto L\rho L^\dagger$ and $g :: \rho \mapsto M\rho M^\dagger$, equation 10 is satisfied:

$$\begin{aligned} f^\dagger \circ f = g^\dagger \circ g &\iff \forall \rho :\ L^\dagger(L\rho L^\dagger)L = M^\dagger(M\rho M^\dagger)M \\ &\iff L^\dagger L = M^\dagger M \\ &\iff \forall \rho :\ tr(L^\dagger L\rho) = tr(M^\dagger M\rho) \\ &\iff \forall \rho :\ tr(L\rho L^\dagger) = tr(M\rho M^\dagger) \\ &\iff \top \circ f = \top \circ g\ . \end{aligned}$$

This example justifies the name ‘environment’: tracing a system out in quantum theory is interpreted as this system being part of the environment.

Example 2. Let $\mathbf{C}$ be any dagger compact category, let $CPM(\mathbf{C})$ the category obtained by applying Selinger’s CPM-construction [35] –we explicitly present this construction in Section 8– and let $WP(\mathbf{C})$ be the category obtained by applying the ‘doubling construction’ of [11] which cancels out ‘abstract global phases’ –cf. Remark 3. Then, the caps of the dagger compact structure provide an environment for $(WP(\mathbf{C}), CPM(\mathbf{C}))$ [12]. When taking $\mathbf{C}$ to be $\mathbf{FHilb}$ then we recover the previous example, with:

$$\mathbf{Dens} = CPM(\mathbf{FHilb}) \qquad \text{and} \qquad \mathbf{Dens^{pure}} = WP(\mathbf{FHilb})\,.$$

Below we assume as given a pair $(\mathbf{C^{pure}}, \mathbf{C})$ with an environment. We set

$$\perp_A := \top_A^\dagger : \mathrm{I} \to A. \tag{12}$$

An element $\psi : \mathrm{I} \to A$ is *normalized* if

$$\top_A \circ \psi = 1_\mathrm{I}\,. \tag{13}$$

Below all elements depicted as triangles are normalized, diagrammatically:

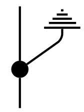
$$= \tag{14}$$

where 1_I is graphically represented by an empty picture.

Proposition 1. [12] *A morphism $f \in \mathbf{C^{pure}}$ is an isometry iff $\top_B \circ f = \top_A$, and hence, it is unitary iff we moreover have that $f \circ \perp_A = \perp_B$.*

6 Classical channels, measurements and classical control

Definition 3. Let Ξ be a classical structure. The morphism:

$C_\Xi =$ 

is called the *classical channel of type* Ξ.

In the light of the discussion in Section 2, this picture can be interpreted as 'copying into the environment', that is, 'broadcasting', or in the decoherence view, 'being coupled to the environment'. Hence, our definition of classical channel enforces broadcastability of the data that it 'transmits'.

Example 3. In **Dens**, for the classical structure of Eqs. (8), we have

$$C_\Xi(\rho) = tr(\Xi_1^2 \circ \rho \circ \Xi_2^1) = \mathcal{D}_{\{|i\rangle\}_i}$$

where $\mathcal{D}_{\{|i\rangle\}_i}$ was defined in Eq. (3).

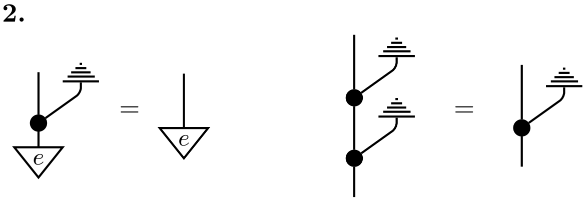
Remark 6. While physically all classical channels are of course the same, our classical channels in addition carry specification of how the classical data it transmits has been obtained, in terms of a dependency on the classical structure Ξ which specifies a particular quantum measurement. In the light of the fact that by default we take all systems to be quantum, this specification of the classical structure relative to which classical data is classical is indeed unavoidable. It is for this reason that we choose to axiomatize the complementary morphism –cf. the discussion in Section 4– which enables us to restrict ourselves to a single classical structure.

The following proposition shows that a classical channel leaves its pure classical elements invariant, and that it is idempotent. In fact, we could define more general *classical elements* $p : \mathrm{I} \to A$ as those that satisfy

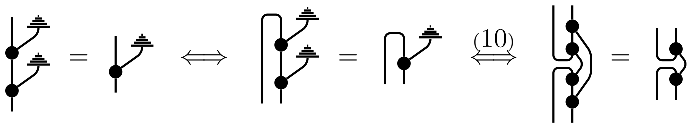
$$C_\Xi \circ p = p\,. \tag{15}$$

Physically, this means that a classical channel 'transmits' its classical elements. Equivalently, classical elements are invariant under decoherence.

Proposition 2.

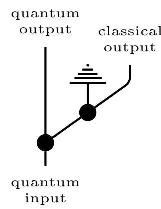


Proof. The first equality follows from Eq. (6) and Eq. (14), and



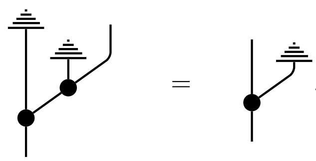
where the last equality holds due to the spider normal form theorem. □

We can now construct a *measurement* as follows:

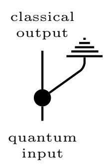


(16)

i.e. it copies the quantum data and specifies that one of the copies is classical; all of this will of course imply that the 'data which flows thorough these wires' will necessarily be decoherent. A *destructive measurement* is obtained by 'feeding the quantum output itself into the environment'. Proposition 2 then yields:

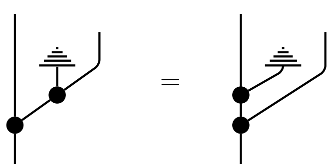


and the resulting shape of the destructive measurement is then:



(17)

Note here in particular that destructive measurements and classical channels are 'semantically equivalent'. Similarly, by the spider normal form we have:

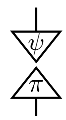


so the quantum output of a measurement is 'semantically equivalent' to its classical output, which captures change of the quantum state to an eigenstate. More generally, as a consequence of the structural power of the spider normal form theorem, classicality 'semantically spreads through a diagram'.

Note that by idempotence of C_Ξ it also follows that $\perp_A = \top_A^\dagger$ is a classical element, and in particular, that this does not depend on the choice of Ξ. We will call $\perp_A$ (unnormalized) *maximal mixedness*.

Example 4. In **Dens** we indeed have that $\perp_{\mathcal{H}}$ is diagonal in any basis.

We call a morphism $f : A \to B$ *disconnected* if it factors along I, that is, if $f = \psi \circ \pi$ for some $\psi : \mathrm{I} \to B$ and $\pi : A \to \mathrm{I}$. In the graphical representation we indeed obtain a disconnected picture in this case:

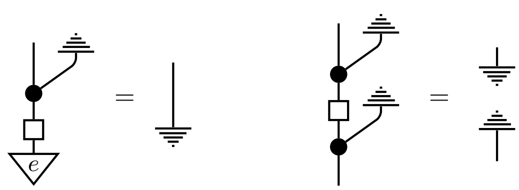


The topological disconnectedness physically stands for the fact that there is no information flowing from the input to the output.

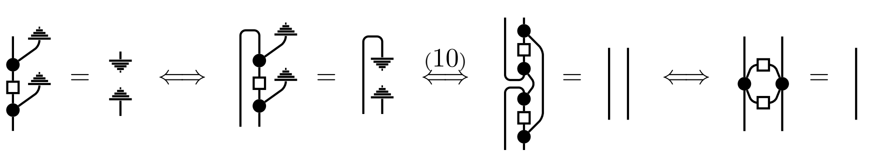
Remark 7. For non-trivial categories the morphisms $\top_A$ cannot be pure; if they would be pure then setting $f := \top_A$ and $g := 1_A$ in Eq. 10, the righthandside becomes $1_{\mathrm{I}} \circ \top_A = \top_A \circ 1_A$, which holds, and hence also the lefthandside holds: $\perp_A \circ \top_A = 1_A \circ 1_A = 1_A$. That is, the identity is 'disconnected'. This is obviously in conflict with the intuition that through a straight wire information flows without being modified, so one expects bad things to happen. Indeed, for any $f : A \to B$ we now have $f = 1_B \circ f \circ 1_A = \perp_B \circ \top_B \circ f \circ \perp_A \circ \top_A = s \cdot \perp_B \circ \top_A$ with $s = \top_B \circ f \perp_A : \mathrm{I} \to \mathrm{I}$ a scalar. That is, any morphism is disconnected!

If we introduce H between C_{Ξ} and itself, we obtain 'complementary behaviors'. The first equality of the following proposition implies that a measurement turns a pure classical element of a complementary measurement in maximal mixedness, i.e. any outcome is equally probable for that measurement (cf. 'unbiasedness'). The second one implies that there is no dataflow from the input to the output when we compose complementary measurements.

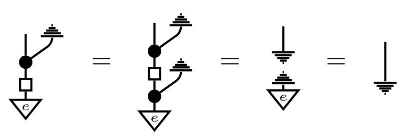
Proposition 3.



Proof. We have



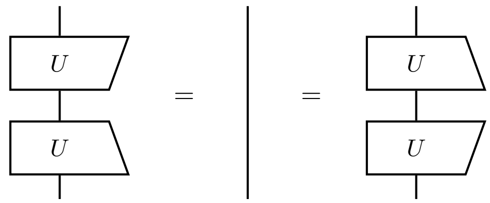
The first equation is derived from the second one and Proposition 2:



$\square$

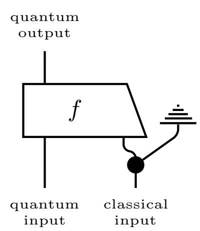
6.1 General classical control operations

In diagrammatic terms, a morphism $U : A \to A$ is unitary if

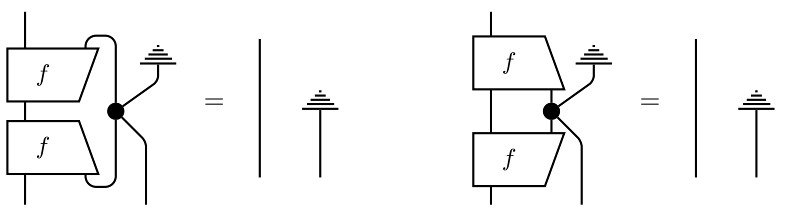


We now define what it means to have a family of unitaries of the same type, 'indexed' by a classical structure, that is, a controlled unitary.

Definition 4. By a *controlled unitary* we mean an operation of the form:



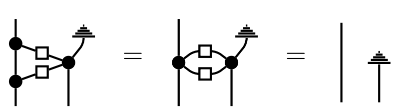
which 'for all classical input values is unitary', that is:



Lemma 1. *The following morphisms are controlled unitaries:*

(18)

Proof. We have



and the remainder of the proof proceeds almost identical. $\square$

6.2 General non-degenerate measurements

We have identified an example of a *non-degenerate measurement*, namely the one of the shape (16), and an example of a *non-degenerate destructive measurement*, namely the one of the shape (17). Relative to a given classical structure we can define more general non-destructive measurements.

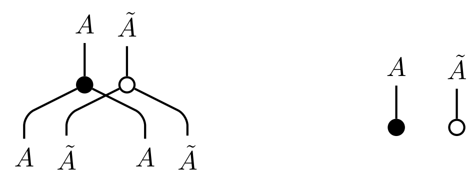
The following Lemma shows how classical data can be composed in terms of classical structures, where we conceive classical structures as being specified by a multiplication and its unit, i.e. $\Xi := (\Xi_2^1, \Xi_0^1)$ –cf. Remark 2.

Lemma 2. [14] *If* (Ξ_2^1, Ξ_0^1) *and* $(\tilde{\Xi}_2^1, \tilde{\Xi}_0^1)$ *are classical structures on* A *and* $\tilde{A}$ *respectively, then the morphisms*

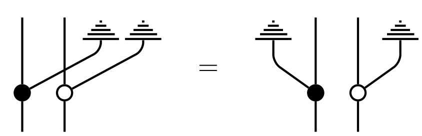
$$(\Xi_2^1 \otimes \tilde{\Xi}_2^1) \circ (1_A \otimes \sigma_{A,\tilde{A}} \otimes 1_{\tilde{A}}) : (A \otimes \tilde{A}) \otimes (A \otimes \tilde{A}) \to A \otimes \tilde{A}$$

$$\Xi_0^1 \otimes \tilde{\Xi}_0^1 : \mathrm{I} \to A \otimes \tilde{A}$$

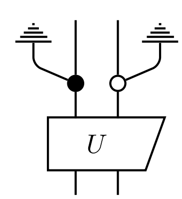
define a classical structure on $A \otimes \tilde{A}$*, diagrammatically,*



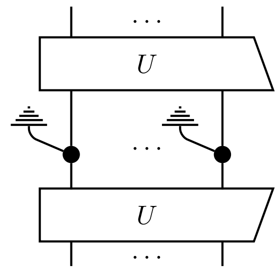
The canonically corresponding non-degenerate destructive measurement which extracts this compound classical data from a pair of quantum systems is:



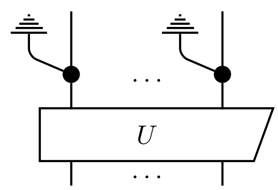
When transforming the quantum data by means of a unitary we obtain the general form of a non-degenerate distructive measurement on a pair of systems:



Definition 5. Given a classical structure on A, a *non-degenerate measurement* on n systems of type A is a morphism of the form:

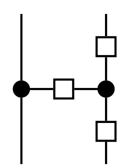


where $U : A \otimes \ldots \otimes A \to A \otimes \ldots \otimes A$ is an arbitrary unitary, and a corresponding *non-degenerate destructive measurement* is a morphism of the form:

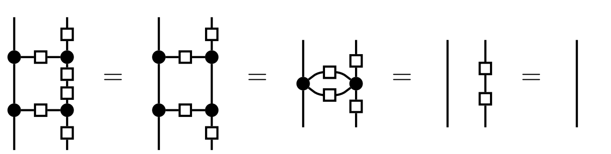


Remark 8. One can also define more general kinds of measurements, namely degenerate ones and non-projective ones, which involves defining projective measurements without reference to unitaries. This can be done in straightforward analogy to how this was done in [20] and [19].

Lemma 3. *The following morphism is unitary:*

$CNOT \quad :=$  (19)

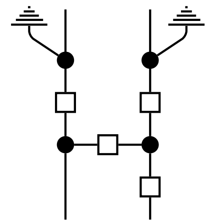
Proof.



□

Corollary 1. *The following morphism is a non-degenerate destructive measurement on a pair of systems of the same type A:*

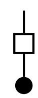
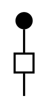
$$Bell\text{-}Meas \quad := $$

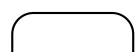


6.3 Interpretation of graphical elements in Dens

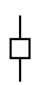
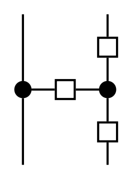
The following tables translate the graphical language to Hilbert space quantum theory for the specific case of qubits. It is this translation which connects that diagrammatic presentation of the protocols in the following section to how one finds them usually described in textbooks.

(pure) states & effects:

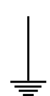
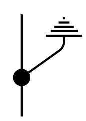
Notation:				
Dens^pure:	$1 \mapsto 2 \cdot \|+\rangle\langle+\|$	$\rho \mapsto 2 \cdot \langle+\|\rho\|+\rangle$	$1 \mapsto 2 \cdot \|0\rangle\langle 0\|$	$\rho \mapsto 2 \cdot \langle 0\|\rho\|0\rangle$

Notation:		
Dens^pure:	$1 \mapsto (\|00\rangle + \|11\rangle)(\langle 00\| + \langle 11\|)$	$\rho \mapsto (\langle 00\| + \langle 11\|)\rho(\|00\rangle + \|11\rangle)$

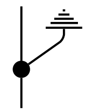
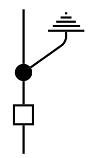
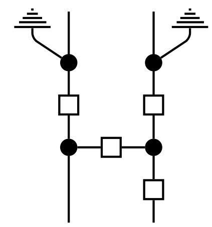
(pure) gates:

Notation:		
Dens^pure:	$\rho \mapsto \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\rho\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	$\rho \mapsto \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\rho\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$

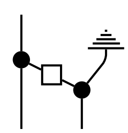
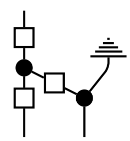
CP maps:

Notation:			
Dens:	trace $\rho \mapsto tr(\rho)$	maximally mixed state $1 \mapsto \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$	erase non-diagonal elements $\rho \mapsto \langle 0\|\rho\|0\rangle + \langle 1\|\rho\|1\rangle$

(destructive) measurements:

Notation:			
Dens:	Pauli Z measurement	Pauli X measurement	Bell-basis measurement

classically controlled operations:

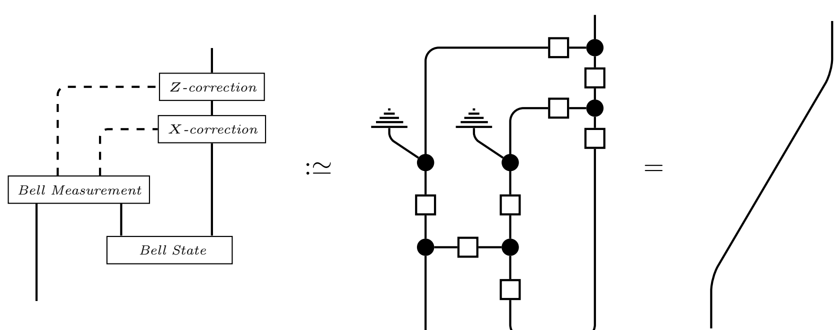
Notation:		
Dens:	Pauli Z correction	Pauli X correction

7 Example protocols

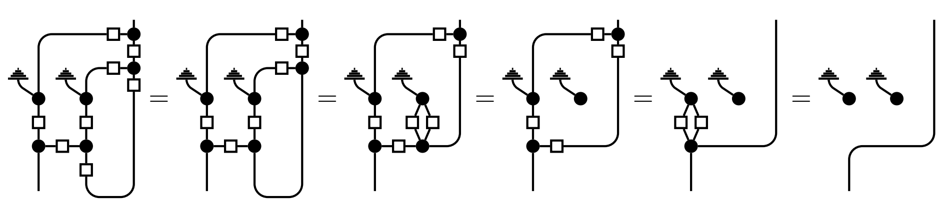
In the statement of each proposition, we will specify protocols with explicit physical types, quantum channels being represented by full lines and classical channels being represented by dotted lines. We use the symbol ':≃' for the passage of this specification to the interpretation within the diagrammatic calculus.

First we show that the teleportation protocol, by means of a Bell state and two classical channels, realizes a (perfect) quantum channel.

Proposition 4 (correctness of teleportation).



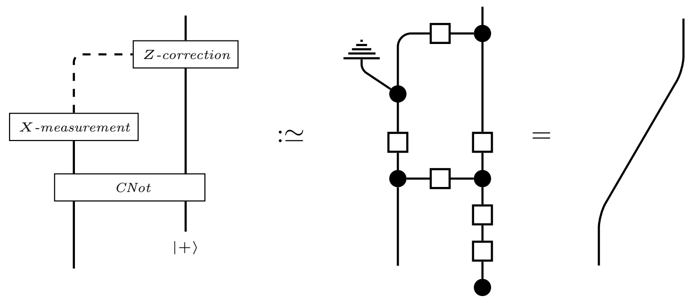
Proof.



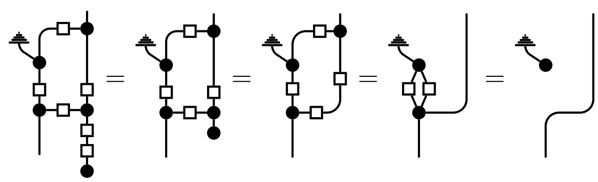
□

We show that the state transfer [34] protocol, by means of 2-qubit unitary tranformation and a local measurement, realizes a (perfect) quantum channel.

Proposition 5 (correctness of state transfer).



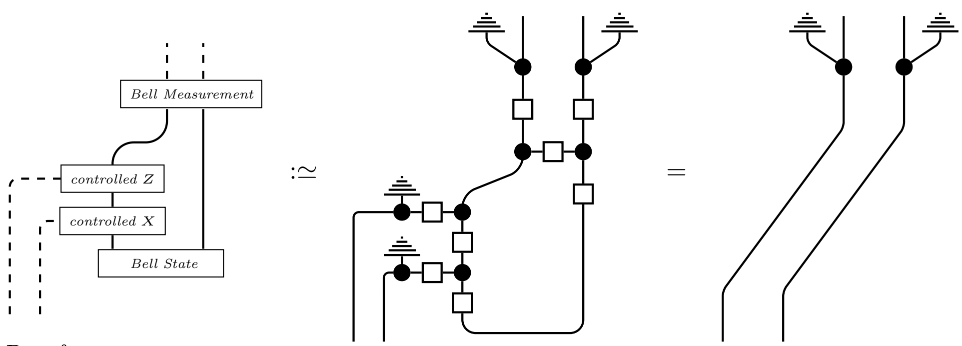
Proof.



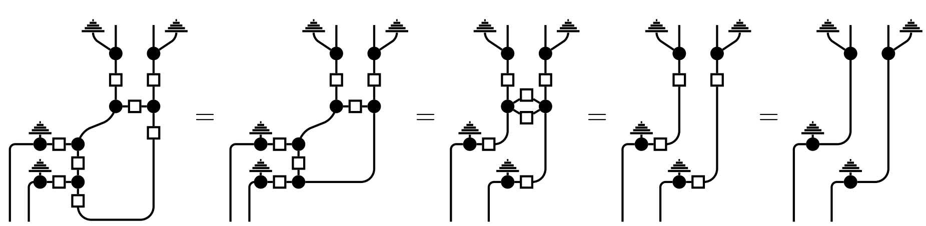
□

Now we show that the dense coding protocol, by means of a Bell state and a quantum channel, realizes two classical channels.

Proposition 6 (correctness of dense coding).



Proof.

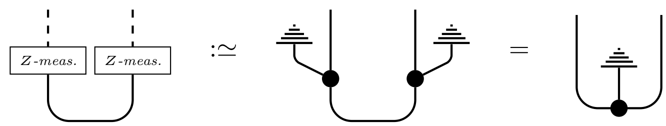


□

A diagrammatic presentation of a key exchange protocols is in [22]. Here we provide a simplified presentation by relying on the notion of environment. We restrict ourselves to four representative cases.

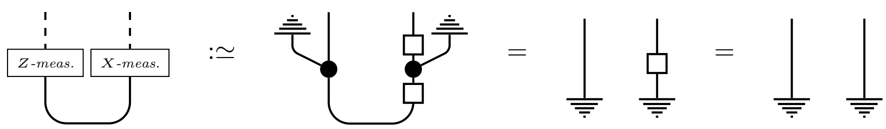
Proposition 7 (correctness of BB84 and Ekert 91 key exchange).

– *Alice and Bob choose the same measurement in Ekert 91:*



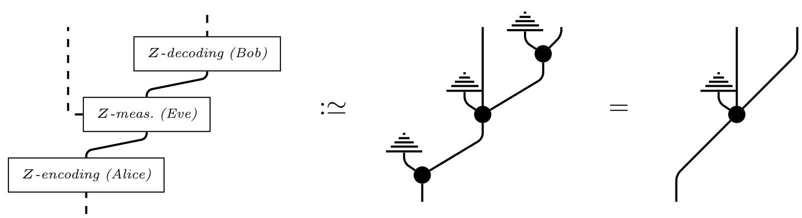
i.e. Alice and Bob share the same classical data.

– *Alice and Bob choose a different measurement in Ekert 91:*



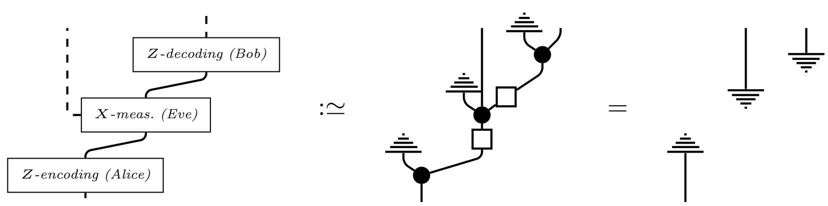
i.e. Alice's and Bob's data is not correlated.

– *Eve chooses the same measurement as Alice and Bob in BB84:*



i.e. Alice, Bob and Eve share the same classical data.

– *Eve chooses a different measurement than Alice and Bob in BB84:*

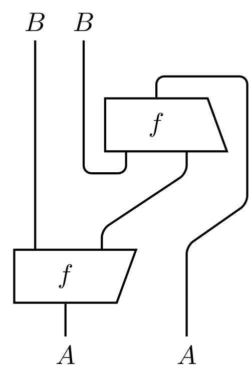


i.e. Alice's, Bob's and Eve's data is not correlated.

8 Connection to Selinger's CPM-contruction

Here we briefly describe the connection of Definition 2 to Selinger's CPM-comstruction [35], which was established in [12]. Given any dagger compact

category $\mathbf{C}$, we define a new category $CPM(\mathbf{C})$ which has the same objects as $\mathbf{C}$, and a morphisms of type $A \to B$ in $CPM(\mathbf{C})$ is a morphism of type $A \otimes A \to B \otimes B$ in $\mathbf{C}$ of the shape:



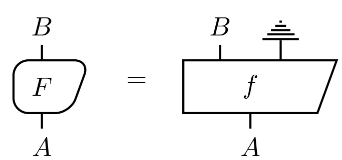
(20)

where $f : A \to B \otimes C$ is any morphism in $\mathbf{C}$. Then, $CPM(\mathbf{C})$ is again a dagger compact category, and as already mentioned in Example 2, if we set $\mathbf{C} := \mathbf{FHilb}$ then the morphisms of the form (20) are exactly completely positive maps.

Definition 6. An *environment with purification* for $(\mathbf{C}^{\mathbf{pure}}, \mathbf{C})$ is an environment as in Definition 2 for which we in addition have that, denoting morphisms in $\mathbf{C}^{\mathbf{pure}}$ and more general morphisms in $\mathbf{C}$ respectively as

,

that for all $A, B \in |\mathbf{C}|, F \in \mathbf{C}(A, B)$ there exists $f \in \mathbf{C}^{\mathbf{pure}}(A, B \otimes C)$ such that



.

Theorem 3. [12] $CPM(\mathbf{C}^{\mathbf{pure}}) = \mathbf{C}$.

As already mentioned in Example 2, the converse statement, that for any dagger compact category $\mathbf{C}$ the category $CPM(\mathbf{C})$ provides an environment with purification also holds, up to a minor and physically justified assumption related to the fact that vectors which are equal up to a complex phase represent the same state in quantum theory. Concretely, this axiom states the for all pure elements $\psi, \psi' : \mathrm{I} \to A$ we have:

$$\psi \circ \psi^\dagger = \psi' \circ \psi'^\dagger \;\Rightarrow\; \psi = \psi' \ .$$

This equation follows from Eq. (10) when setting $f := \psi^\dagger$ and $g := \psi'^\dagger$.

Remark 9. The power of a purification axiom has recently been exploited in [9,10], although there, the authors also require certain uniqueness properties.

9 Conclusion

An axiomatization of the concept of environment resulted in a very simple comprehensive graphical calculus, which in particular enables one to reason about classical-quantum interaction in quantum informatic protocols.

Several operationally distinct concepts turn out to have the same semantics within the graphical language (e.g. classical channel, measurement, preparation as in BB84). Consequently, all that one structurally truly needs are Propositions 2 and 3 on composition of classical channels and pure classical elements.

The examples given here are simple but representative. This work and the earlier contributions on which we relied together successfully addresses a challenge for the categorical quantum mechanics research program which was set at the very beginning: to have a very simple graphical description of all basic quantum informatic protocols, in particular including classical-quantum interaction.

The new graphical element 'environment' and the interaction rules for classical channels can now be integrated in the `quantomatic` software [24], so that it can now be used to (semi-)automate reasoning about full-blown quantum informatic protocols, including classical-quantum interaction.

Here we only considered two complementary observables. We meanwhile also have graphical calculi that are universal for quantum computing [14,16]. The next step of this research strand would be to extend the graphical calculus presented here to these calculi, which include, for example, phases and W-states.

This work could also be advanced in the direction of quantum information theory. In particular, one may want to study whether it would be possible to obtain a diagrammatic account on quantum informatic quantities. Some examples of diagrammatic quantum informatic quantities are in [12].

References

1. S. Abramsky (2009) *No-cloning in categorical quantum mechanics.* In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 1–28, Cambridge University Press. arXiv:0910.2401
2. S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols.* In: Proceedings of 19th IEEE conference on Logic in Computer Science (LiCS), pages 415–425. IEEE Press. arXiv:quant-ph/0402130. Revised version (2009): *Categorical quantum mechanics.* In: Handbook of Quantum Logic and Quantum Structures, K. Engesser, D. M. Gabbay and D. Lehmann (eds), pages 261–323. Elsevier. arXiv:0808.1023
3. S. Abramsky and B. Coecke (2005) *Abstract physical traces.* Theory and Applications of Categories **14**, 111–124. arXiv:0910.3144
4. H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher (1996) *Non-commuting mixed states cannot be broadcast.* Physical Review Letters **76**, 2818–2821. arXiv:quant-ph/9511010

5. C. H. Bennett and G. Brassard (1984) *Quantum cryptography: Public key distribution and coin tossing*. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179.
6. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters (1993) *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Physical Review Letters **70**, 1895–1899.
7. C. H. Bennet and S. Wiesner (1992) *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*. Physical Review Letters **69**, 2881–2884.
8. A. Carboni and R. F. C. Walters (1987) *Cartesian bicategories I*. Journal of Pure and Applied Algebra **49**, 11–32.
9. G. Chiribella, G. M. D'Ariano and P. Perinotti (2009) *Probabilistic theories with purification*. Physical Review A **81**, 062348. arXiv:0908.1583
10. G. Chiribella, G. M. D'Ariano, and P. Perinotti (2010) *Informational derivation of quantum theory*. arXiv:1011.6451
11. B. Coecke (2007) *De-linearizing linearity: projective quantum axiomatics from strong compact closure*. Electronic Notes in Theoretical Computer Science **170**, 47–72. arXiv:quant-ph/0506134
12. B. Coecke (2008) *Axiomatic description of mixed states from Selinger's CPM-construction*. Electronic Notes in Theoretical Computer Science **210**, 3–13.
13. B. Coecke and R. Duncan (2008) *Interacting quantum observables*. In: Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP), pp. 298–310, Lecture Notes in Computer Science 5126, Springer-Verlag.
14. B. Coecke and R. Duncan (2011) *Interacting quantum observables: categorical algebra and diagrammatics*. arXiv:0906.4725.**v2**
15. B. Coecke, B. Edwards and R. W. Spekkens (2010) *Phase groups and the origin of non-locality for qubits*. Electronic Notes in Theoretical Computer Science, to appear. arXiv:1003.5005
16. B. Coecke and A. Kissinger (2010) *The compositional structure of multipartite quantum entanglement*. In: Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP), pp. 297–308, Lecture Notes in Computer Science 6199, Springer-Verlag. arXiv:1002.2540
17. B. Coecke and E. O. Paquette (2009) *Categories for the practicing physicist*. In: New Structures for Physics, B. Coecke (ed), pages 167–271. Lecture Notes in Physics, Springer-Verlag. arXiv:0905.3010
18. B. Coecke, E. O. Paquette and S. Perdrix (2008) *Bases in diagrammatic quantum protocols*. Electronic Notes in Theoretical Computer Science **218**, 131–152. arXiv:0808.1037
19. B. Coecke, E. O. Paquette and D. Pavlovic (2009) *Classical and quantum structuralism*. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 29–69, Cambridge University Press. arXiv:0904.1997
20. B. Coecke and D. Pavlovic (2007) *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 567–604. Taylor and Francis. arXiv:quant-ph/0608035.
21. B. Coecke, D. Pavlovic, and J. Vicary (2011) *A new description of orthogonal bases*. Mathematical Structures in Computer Science, to appear. arXiv:0810.0812
22. B. Coecke, B.-S. Wang, Q.-L. Wang, Y.-J. Wang and Q.-Y. Zhang (2010) *Graphical calculus for quantum key distribution*. Electronic Notes in Theoretical Computer Science, to appear.
23. D. G. B. J. Dieks (1982) *Communication by EPR devices*. Physics Letters A **92**, 271–272.

24. L. Dixon, R. Duncan, A. Kissinger and A. Merry, `quantomatic` software tool, http://dream.inf.ed.ac.uk/ projects/quantomatic/
25. L. Dixon and A. Kissinger (2010) *Open graphs and monoidal theories*. arXiv:1011.4114
26. R. Duncan and S. Perdrix (2009) *Graph states and the necessity of Euler decomposition*. In: Proceedings of Computability in Europe: Mathematical Theory and Computational Practice (CiE'09), pages 167–177. Lecture Notes in Computer Science 5635, Springer-Verlag. arXiv:0902.0500
27. R. Duncan and S. Perdrix (2010) *Rewriting measurement-based quantum computations with generalised flow*. In: Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP), Lecture Notes in Computer Science 6199, Springer-Verlag.
28. A. Ekert (1991) *Quantum cryptography based on Bell's theorem*. Physical Review Letters **67**, 661–663.
29. A. Joyal and R. Street (1991) *The Geometry of tensor calculus* I. Advances in Mathematics **88**, 55–112.
30. G. M. Kelly and M. L. Laplaza (1980) *Coherence for compact closed categories*. Journal of Pure and Applied Algebra **19**, 193–213.
31. S. Lack (2004) *Composing PROPs*. Theory and Applications of Categories **13**, 147–163.
32. S. Mac Lane (2000) *Categories for the Working Mathematician* (2nd edition), Springer-Verlag.
33. R. Penrose (1971) *Applications of negative dimensional tensors*. In: Combinatorial Mathematics and its Applications, D. Welsh (Ed), pages 221–244. Academic Press.
34. S. Perdrix (2005) *State transfer instead of teleportation in measurement-based quantum computation*. International Journal of Quantum Information **3**, 219–223. arXiv:quant-ph/0402204
35. P. Selinger (2007) *Dagger compact closed categories and completely positive maps*. Electronic Notes in Theoretical Computer Science **170**, 139–163.
36. P. Selinger (2009) *A survey of graphical languages for monoidal categories*. In: New Structures for Physics, B. Coecke (ed), 275–337, Springer-Verlag. arXiv:0908.3347
37. P. Selinger (2010) *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. Electronic Notes in Theoretical Computer Science, to appear. http://www.mscs.dal.ca/∼selinger/papers/finhilb.pdf
38. P. Selinger (2010) *Autonomous categories in which A is isomorphic to A^**. In: Proceedings of the 7th International Workshop on Quantum Physics and Logic (QPL 2010), Oxford. http://www.mscs.dal.ca/∼selinger/papers/halftwist.pdf
39. W. K. Wootters and W. Zurek (1982) *A single quantum cannot be cloned*. Nature **299**, 802–803.
40. W. H. Zurek (1991) *Decoherence and the Transition from Quantum to Classical*. Physics Today **44**, 36–44. arXiv:quant-ph/0306072